TAMPEREEN
AMMATTIKORKEAKOULU

CISCO TRUSTSEC TIETOVERKON SEGMENTOINNISSA

Jari-Pekka Pöllänen

Opinnäytetyö
Elokuu 2018
Tietotekniikan koulutusohjelma
Sulautetut Järjestelmät

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Sulautetut Järjestelmät

PÖLLÄNEN JARI-PEKKA
Ciscon TrustSec verkon segmentoinnissa

Opinnäytetyö 21 sivua
Elokuu 2018

Opinnäytetyön tarkoitus on selventää kuinka jatkuvasti kehittyvät ja monipuolistuvat uhat sähköisille palveluille tapahtuvat nopeudella, joka on toista luokkaa kuin muissa perinteisissä palveluissa. Tämän opinnäytetyön tavoite on ollut tutkia kuinka Cisco TrustSec teknologiaa voidaan hyödyntää eri yritysten verkon segmentoinnissa.

Cisco TrustSec mahdollistaa ratkaisun tulevaisuudessa lisääntyvien laitteiden ja kasvavan verkon segmentointiin liittyvissä ongelmissa. Tietoturvallisuus täytyy parantua ja muuttua helpommin hallittavaksi laitteiden lisääntyessä vanhojen hallinnointitapojen muuttuessa turhan monimutkaisiksi kehityksen edetessä. Maksutietovälineitä välittävä ja hallinoiva yritys joutuu panostamaan nykyisten tapahtuneiden kaappausten ilmennyttyä omaan tietoturvaansa, turvatakseen asiakkaat ja palveluntoimittajat näiltä hyökkääjiltä. Ciscon teknologia tarjoaa päivityksen vanhalle lähestymistavalle tietoverkon hallinnointiin ja ylläpitoon liittyen, heidän omilla laitteilla jotka tukevat teknologiaa tai yrityksen omilla laitteilla joissa tukea teknologialle ei löydy.

Tutkielman asetetut tavoitteet saavutettiin ja ymmärrys tulevaisuuden maksuvälineliikennettä hallinoivan yrityksen ja muiden yritysten tietoverkon segmentointiin liittyvät haasteet ja ratkaisut tulevat selväksi.

Asiasanat: segmentointi, tietoverkko, TrustSec, PCI

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Information & Computer Technology
Embedded systems

PÖLLÄNEN JARI-PEKKA SAKARI
Cisco TrustSec in network segmentation

Bachelor's thesis 21 pages
August 2018

Subject of this thesis is to clarify in what speed continuously developing and diversifying threats are to online services, that they are in a another level while comparing to traditional services. The goal of this thesis is to inspect how Cisco TrustSec technology can be used in various companies network segmentation.

Cisco TrustSec enables solution for the future, when the amount of end devices are increasing and segmentation problems in expanding networks. Network security has to become better and change to easily controllable, despite the continuous increase in end-devices and when old solutions are becoming too complex to be administrated. Company that stores and uses payment card data has to invest in network security due to the customer information leaks that have happened lately, to secure their customers and their information from these threats. Cisco's technology provides an update to the old way to do network segmentation and handling the network. Cisco's technology can be used through their own devices or with their technology protocol also old devices can be deployed.

The goals that were set to this thesis were all achieved and the knowledge and understanding regarding future challenges in payment card data handling and company's network segmentation challenges and solutions come clear in this thesis.

Key words: segmentation, network, TrustSec, PCI

SISÄLLYS

LYHENTEET JA TERMIT (valitse jompikumpi)

ARP	Address Resolution Protocol
SGT	Security Group Tag
SGA	Security Group Access
ACL	Access List
IP-osoite	Internet protocol-osoite
MAC-osoite	Media Access Control -osoite
VLAN	Virtual Local Area Network
OSI-malli	Open Systems Interconnection -malli
TCAM	Ternary Content-Addressable Memory
POS	Point of Sale
PCI-DSS	Payment Card Industry Data Security Standard
SSID	Service Set Identifier
WLAN	Wireless Local Area Network
SSO	Single Sign-On
ACE	Access Control Enfrocement
DHCP	Dynamic Host Control Protocol

1 JOHDANTO

Lähiverkkoa voidaan suojata erilaisilla tavoilla, verkon pystyy segmentoimaan erilaisiin turva-alueisiin, rajoittaa verkkoon liittymistä, reititysprotokollien suojaaminen, toisin sanoen mahdollisuuksia on monia erilaisia. Työn tarkoituksena on selvittää kuinka Cisco SGT auttaa tietoverkon tietoturvan parantamisessa.

Tutkimuksen pohjana toimii, kuinka tietoverkon segmentointia voidaan pelkistää ja turvata lisäämättä enemmän VLAN:eja. Yksi tärkeimmistä asioista on, kuinka toiminnallinen palomuurien hallinta ja käyttöoikeuksien hallinoiminen voidaan pelkistää.

Tutkimuskysymyksinä ovat Kuinka kasvava tietoverkko pystytään pitämään turvallisena ja helposti hallittavana? ja Kuinka estää luvaton pääsy verkon sisällä ilman käyttöoikeuksia? Työn tavoitteena on selventää tietoverkon segmentoinnin hallinnoinnin pelkistäminen ja tietoturvan parantaminen.

Opinnäytetyössä on tietoperusta, jossa peruskäsitteet käydään läpi. Tämän jälkeen on tietoverkon segmentointi selitettynä, josta selvyyden vuoksi otetaan esimerkkinä yritys joka käsittelee maksukorttitietoja omassa tietoverkossa.

2 TIETOPERUSTA

Tutkielmassa on käytetty useita eri tietolähteitä. Seuraavassa osiossa selitetään tutkielmaan liittyvät peruskäsitteet ja toiminta.

Cisco TrustSec on Ciscon kehittämä ohjelmisto määritelty segmentointi, joka dynaamisesti järjestelee päätepisteet loogisiin ryhmiin, joita kutsutaan suojatuiksi ryhmiksi (security groups). Suojatut ryhmät määritelty yrityspäätösten muodossa, käyttäen rikkaampaa kontekstia kuin IP-osoite. Suojatut ryhmät ovat helpompia ihmisten ymmärtää ja hallita. Suojattujen ryhmien sääntöjen määrät ovat huomattavasti vähäisempiä, kuin vastaavat säännöt IP-osoitteilla. (”Cisco TrustSec Software-Defined Segmentation”, Cisco 2017)

SGT on turvallisuustunniste joka määrittelee käyttäjän käyttöoikeudet kyseisessä tietoverkossa.

Virtuaalilähiverkko (engl. VLAN) on tapa jolla voidaan jakaa fyysinen tietoliikenneverkko loogisiin osiin. Käytännössä virtuaalilähiverkko tarkoittaa sitä, että yrityksen eri osastot voidaan jakaa omiin verkkoihin riippumatta miten osastot ovat jaoteltuna rakennuksen sisällä.

Aliverkko (engl. Subnet) on tietokoneverkon looginen osa, se sijaitsee OSI-mallin kolmannella kerroksella. Aliverkotus on termi, jota käytetään kun suurempi verkko pilkotaan pienempiin osiin. Käytännössä IP-osoitteet jaetaan eri loogisille verkkokokonaisuuksille.

Segmentointi, tietoliikenneverkossa segmentointi tarkoittaa, kun osa tietoliikenneverkosta on erotettu omaksi verkoksi, esimerkiksi laitteella kuin kytkin tai reititin.

Lähiverkko (LAN) on tietokoneverkko, joka yhdistää eri päätelaitteita rajatun alueen sisällä, kuten omakotitalo, koulu, yliopiston kampus tai toimistorakennus. Lähiverkon perusperiaate on että useammalla päätelaitteella on pääsy verkon sisällä oleviin kohteisiin ja dataa pystytään lähettämään jatkuvasti. Tyypillisin keskustelu metodi jota käytetään lähiverkossa on Ethernet.

Ethernet kehys, dataa liikutetaan päätelaitteelta toiselle lähiverkoissa ethernet-kehyksissä. Kehys koostuu seuraavista osista aloittaen ensimmäisestä, lähde- ja kohdeosoitteen otsakkeista, seuraavaksi tulee hyötykuorma eli lähetettävä ip-paketti ja tarkistussumma.

MAC-osoite on verkkosovittimen ethernet-verkossa yksilöivä tunniste. Useasti päätelaitteen MAC-osoite on kirjattu fyysisesti laitteen takalevyyn. Osoite muodostuu kuudesta kaksinumeroisesta heksadesimaalisesta luvusta, joista ensimmäiset kolme kertovat valmistajan ja loput ovat juoksevia numeroita.

IP-osoite on sarja numeroita mitä käytetään IP-verkkoihin kytkettyjen verkkosovittimien yksilöimiseen. Internet protokollaosoite on alin yhtenäinen Internetin protokolla, myös kaikki data internet-verkon tietoliikenteessä kulkee IP-paketteina. IP-osoitteen avulla IP-paketit löytävät perille ja saavat vastauksensa takaisin.

OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmää seitsemässä eri kerroksessa. Mallin tarkoituksena on antaa selkeä käsitemalli ymmärtämiseen, suunnitteluun ja kehittämiseen. Jokainen OSI-mallin kerroksista kommunikoi alemman kerroksen viesteihin rakennettujen rajapintojen avulla.

PCI-DSS, Payment Card Industry Data Security Standard on maksukorttialan tietoturvastandardi. Standardin tarkoituksena on määritellä maksukortti ympäristön säännöt jossa jälleenmyyjät ja palveluntarjoajat käsittelevät ja säilyttävät korttitietoja.

Kytkin on laite jolla yhdistetään pakettikytkennäisien paikallisverkkojen osia toisiinsa.’

TCAM on erikoistunut suuri nopeuksinen muisti tyyppi, joka etsii kokonaan sen sisällön yhdellä kellopulssilla.

SGA on ratkaisu joka luo pilven luotetuille tietoverkonlaitteille ja samalla rakentaa turvallisen ympäristön tietoverkoille.

SXP, Ciscon Security Exchange Protocol (SXP) tai toiselta nimeltä SGT Exchange Protocol (SXP) on Ciscon SGA-palvelua varten kehitetty protokolla niille laitteille jotka eivät ole turvallisuustunniste yhteensopivia.

POS on järjestelmä, joka voi olla yksinkertaisen kassakoneen ja tietokoneelle tai palvelimelle dataa tallentavan tietokonepohjaisen järjestelmän väliltä. Toisin sanoen laite missä myyntitapahtuma käsitellään.

SSID on lyhenne sanoista Service Set Identifier, jolla tarkoitetaan langattoman lähiverkon tunnusta. SSID toimii saman alueen WLAN-verkkojen erottelijana.

ARP(Address Resolution Protocol) on protokolla jolla selvitetään verkkokortin MAC-osoite tunnetusta IP-osoitteesta. Lähiverkossa laitteet käyttävät liikennöinnissä MAC-osoitteita ja reititinverkossa käyttäen IP-osoitteita.

Trunk-portti on portti joka kuljettaa usean VLAN:in kehyksiä eri kytkimien välillä. Toisin sanoen monia virtuaalilähiverkkoja ketjutetaan fyysisesti eri pisteiden välillä.

VLAN hyppely on yleisimmin käytetty termi kun kaksi 802.1Q Ethernet-kehystä paketoidaan sisäkkäin ja päästään tämän avulla käsiksi toiseen VLANiin. Mutta myös muita menetelmiä joissa edetään VLANista toiseen ilman oikeuksia ilmaistaan välillä VLAN hyppelynä.

Hyökkääjä tai toiselta nimeltään hakkeri, tarkoittaa tietojärjestelmiin murtautuvaa henkilöä. Yleensä nämä edellä mainitut mielletään pahaa tekeviksi henkilöiksi, mutta on myös henkilöitä jotka tekevät näitä selvittääkseen ongelma-kohtia esimerkiksi eri palveluntarjoajien palveluista.

Pilvi tai pilvipalvelu on kun tietojen säilytys ja käyttö tai ohjelmisto sijaitsee ulkopuolisella palvelimella, eikä käyttäjän omalla tietokoneella.

Kryptaus eli salaus on prosessi jossa viesti tai tieto koodataan sitten, että vain osapuoli jolla on valtuuted voi lukea sen.

DHCP eli Dynamic Host Control Protocol mahdollistaa IP-osoitteen hakemisen ADSL-operaattorilta ja sen jakamisen DHCP- ja NAT-toiminnolla sisäverkkoon. DHCP on keino, jolla verkotetut tietokoneet voivat saada TCP/IP-osoitteensa keskuskoneelta.

3 SEGMENTOINTI

Verkon segmentoinnilla tarkoitetaan, missä tietoverkko jaetaan pienempiin verkko segmentteihin. Segmentoinnilla erotetaan järjestelmän ryhmät tai applikaatiot toisistaan, joka mahdollistaa tietoturva valvontapäätteiden sallia tai evätä liikenteen näiden välillä.

Perinteisessä tietoverkossa tämä toisistaan erilleen erottaminen käyttää käyttöoikeuksia, jotka pohjautuvat verkko-osoitteisiin, VLAN:eihin ja palomuureihin. Yritykset voivat täten ohjata täytäntöönpanoa kuinka liikennettä hallitaan näiden erillisten segmenttien välillä.

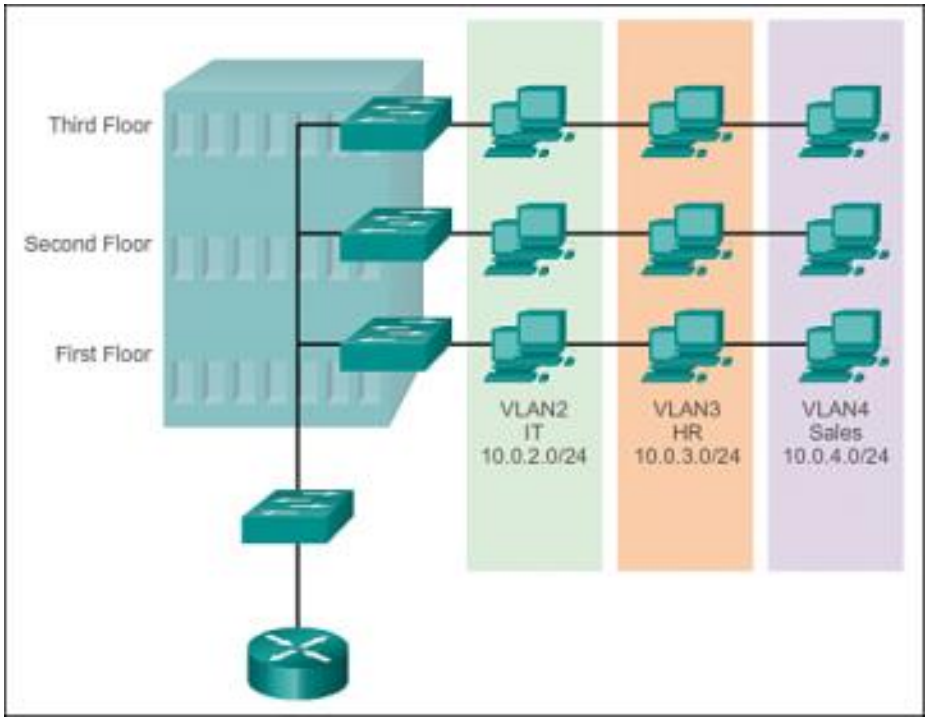
Segmentointi pystytään tekemään, joko fyysisesti tai virtuaalisesti, lopputuloksen ollessa samankaltainen. Tarkoituksena on rajoittaa kommunikointia tietoverkon sisällä, joka rajoittaa mahdollisia hyökkäys menetelmiä. Segmentointi mahdollistaa tietoverkon ongelmien eristämisen, parantaa tietoverkon suorityskykyä, maksimoi olemassaolevaa kaistanleveyttä ja ratkaisee tietoverkon ruuhkautumiseen liittyviä ongelmia. Selven nykseksi segmentointi mahdollistaa laitteisto ja ohjelmisto vikojen pysymisen kyseisen segmentin sisällä, sen sijaan että nämä viat vaikuttaisivat koko tietoverkkoon (Sabina Piyevsky, 2015).

Tutkielmassa on otettu erityissyyniin maksukorttien datan(PCI data) turvaaminen segmentoinnilla. Ensimmäinen asia joka huomioidaan segmentoinnissa, kun toteutetaan PCI data turvallisuus standardin mukainen verkko on verkon rajaus. Tässä prosessissa tunnistetaan kaikki järjestelmän komponentit jotka sijaitsevat tai olevat samassa ympäristössä kuin maksukortti data. Rajaus on yrityksen jokavuotinen tehtävä ennen vuosittaista arviointia. Vähittäiskauppojen ja muiden yhteisöjen täytyy tunnistaa kaikki maksukortti datan liikenne ja sijainti varmistuakseen että jokainen tähän tietoon pääsevä kuuluu PCI data turvallisuus standardin rajaukseen. (PCI Security Standards Counsil)

3.1 Virtuaalilähiverkko

VLAN eli virtuaalilähiverkko on looginen aliverkko joka mahdollistaa ryhmän eri päätelaitteita saman verkon alle, vaikka nämä laitteet fyysisesti sijaitsisivat eri lähiverkoissa.

Ilman virtuaaliverkkoa, esimerkiksi ison rakennuksen samassa kerroksessa ja samaan kytkimeen liitetyt laitteet pystyisivät keskustelemaan keskenään, mahdollistaen käyttäjien selvittää toisen osaston palveluja ja nuuskia datapaketteja.



KUVA 1. VLAN toteutettuna monikerroksiseen rakennukseen.(©2018 Pearson Education, Cisco Press.)

Kuvassa (KUVA 1) nähdään kolme kerroksinen rakennus, jossa jokaisessa kerroksessa on oma kytkin, johon päätelaitteet ovat kytkettynä. Kaikissa kerroksissa on yrityksen eri osastojen käyttäjiä, jotka ovat fyysisesti jokaisen kerroksen kytkimeen yhteydessä, mutta kuuluvat omiin virtuaaliverkkoihin, jotka ovat esitettynä eri väreillä. Vihreä kuuluu IT-henkilöstölle, oranssi henkilöstöhallinnolle ja lila myyntihenkilöstölle. Järjestelmän haltija pystyy luomaan omat virtuaaliverkot erillisille osastoilleen riippumatta siitä olisivatko ne fyysisesti suoraan yhteydessä toisiinsa. Kerroksien välillä on kuitenkin kytkimien välillä yhteys, mutta kytkimien portit ovat osoitettu omiksi virtuaalilähiverkoiksi, joihin käyttäjät ovat kytkeytyneet. Virtuaalilähiverkko mahdollistaa verkon segmentoimisen eri osiin, jolloin evätään pääsy osastojen välillä, mihin toisen osaston ei tulisi olla yhteydessä aiheuttaakseen tietoturvauhkaa.

3.2 Staattinen ja dynaaminen VLAN

On olemassa kahdenlaista virtuaalilähiverkkoa, staattinen ja dynaaminen. Molemmat virtuaalilähiverkkoja voidaan käyttää kattamaan pienen tai suuren maantieteellisen alueen.

3.2.1 Staattinen virtuaalilähiverkko

Staattinen virtuaalilähiverkko josta käytetään nimitystä porttipohjainen virtuaalilähiverkko. Staattisessa virtuaalilähiverkossa kytkimien portit täytyy manuaalisesti osoittaa omaksi virtuaalilähiverkoksi. Päätelaitteesta tulee kyseisen portin virtuaalilähiverkon jäsen johon se kytketään, jonka määrittää mille virtuaalilähiverkolle fyysinen portti on kytkimessä osoitettu. Yhdessä kytkimessä voi olla useampi virtuaalilähiverkko osoitettuna eri porteille, mutta liikennettä näiden porttien välillä ei tapahdu, koska ne kuuluvat eri virtuaaliverkkoihin (Shabeer ibm, 2014).

3.2.2 Dynaaminen virtuaalilähiverkko

Dynaamisessa virtuaalilähiverkossa kytkin automaattisesti osoittaa portin omaan virtuaalilähiverkkoon, käyttäen tietoja päätelaitteesta kuin MAC-osoitetta, IP-osoitetta, jne. Kun päätelaite on kytketty kytkimen porttiin, kytkin tekee kyselyn tietokantaan vahvistaakseen virtuaalilähiverkon jäsenyyden. Verkon järjestelmävalvojan täytyy konfiguroida virtuaalilähiverkkojen tietokanta virtuaalilähiverkon jäsenmenettely serverillä (VMPS, VLAN Membership Policy Server). Dynaaminen virtuaalilähiverkko tukee päätelaitteen välitöntä liikkuvuutta, kun päätelaite vaihdetaan kytkimen portista toiseen kytkimen porttiin, dynaaminen virtuaalilähiverkko automaattisesti konfiguroi oikean virtuaalilähiverkko-jäsenyyden (Shabeer ibm, 2014).

3.3 VLAN ongelmat

Tietoverkkojen järjestemänvalvojat ovat hyödyntäneet virtuaalilähiverkkoja datan suojauksessa, erotellessaan OSI-mallin toista kerrosta. Virtuaalilähiverkon tunnisteiden lisäämistä ei suunniteltu tietoturva toimenpiteeksi. Tavanomaiset segmentointi menetelmät ovat järjestelmällisesti ja hallinnollisesti hyvin kompleksisia. Täytyy skaalata tietoverkkoa jatkuvasti ja ylläpitää pääsyoikeuksien valvontaa kriittisiin tietoverkon osiin datakeskuksessa samalla kuin tilannetietoisuutta täytyisi parantaa jatkuvasti. Määrällisesti jatkuva kasvu rooleissa ja päätelaitteiden määrässä organisaatioiden sisällä, virtuaalilähiverkkojen ylläpito kustannukset kohoavat kovalla vauhdilla.

VLAN segmentoimisen turvallisuus ei vastaa yksinään tämänpäivän vaatimuksia saati huomisen, esimerkkinä VLAN hyppely. VLAN hyppely on yleisin termi liittyen mihin tahansa tapaan jolla saastunut päätelaite saadaan lähettämään paketteja virtuaalilähiverkon porttiin johon sillä ei pitäisi olla mitään pääsyä normaalisti. Saastunut päätelaite voi ohittaa virtuaalilähiverkon tietoturvan tietämällä jonkin laitteen MAC-osoitteen, joka kuuluu kyseiseen järjestelmään. Tämän kaltaisen tietoturva uhan mahdollistaa jos kyseinen hyökkääjä tietää järjestelmän laitteesta ja sen sijainnista, jota yritetään käyttää hyökkäystä varten. Hyökkääjän tietäessä laitteen MAC-osoitteen, hän pystyy syöttämään hyökättävään järjestelmän laitteelle staattisia osoitteita ja paikalliseen ARP välimuistiin. Tämä mahdollistaa suoran kommunikoinnin laitteiden välillä vaikka sijaitsisivat eri virtuaalilähiverkoissa. Kytkimet käyttävät trunk-portteja luodakseen kanavan kommunikoinnille, joka mahdollistaa virtuaalilähiverkkojen alueen useammalle kytkimelle. Kun kytkin kytketään olemassa olevaan lähiverkkoon se kytketään trunk-portin kautta. Data paketit lähetetään kytkimeltä toiselle VLAN-tunnisteella varustettuna, joten jokaisen paketin virtuaalilähiverkon määränpää on hallittua ja liikenne eroteltu muusta liikenteestä. Trunk-ketjuttaminen voidaan konfiguroida porttipohjaiseksi white tai black listan mukaan, riippuen myös laitetoimittajan implementoinnista. Kytkinten käyttäessä trunk-ketjutusta luodakseen kommunikaatiokanavan kytkimien välille, käyttöoikeuden vioittuessa voi johtaa saastuneen laitteen ilmestymisen kytkimenä joka vaatii trunk-yhteyden tietoverkkossa muiden tavallisten kytkimien kaltaisesti. Virtuaalilähiverkossa trunk-portti on portti jolla on potentiaalisesti pääsy kaikkiin sille sallittuihin virtuaalilähiverkkoihin. Saastuneen päätelaitteen ollessa kytkeytyneenä trunk-portissa, se voisi yrittää hyppiä virtuaalilähiverkkojen välillä lähettämällä paketin laitteelle tai portille joka olisi varustettu samalla VLAN-tunnisteella toisessa virtuaalilähiverkossa johon sillä normaalisti ei olisi pääsyä (Steve A. Rouiller, SANS Institute, 8-10, 2013).

4 CISCO TRUSTSEC

Identiteettipohjaisten verkkoyhteyksien konsepti tarjoaa valtuuksia luoda yhteyden tietoverkkoon tai resurssiin. Vuosien saatossa tämä ilmiö on muuttunut jatkuvasta sisäänkirjautumisesta yksittäiseen sisäänkirjautumiseen(single sign-on,SSO) ja keskitettyihin käyttäjärekistereihin jotka käyttävät useita autentikointi metodeja ja vahvistettuihin valtuutusmenettelyihin. Security Group Access antaa pääsyn tietoverkon resursseihin identiteetin ja yhdistyneiden menettelytapojen kautta, parantaa tietoturvaa ja helpottaa datan kulkemisen segmentointia, vähentää kustannuksia ja isojen sekä monimutkaisten palomuurien ja käyttöoikeuslistan sääntöjen väheneminen helpottavat tietoverkon hallintaa, tarjoaa mekanismin johdonmukaisen ja dynaamisen menettelytavan eri alustoilla ja mahdollistaa keskitettyjen menetteltapojen hallinnan ja auditoinnin jokaiselle identiteetille. SGA perustuu ryhmien turvallisuustunnisteisiin (Natalie Timms, 2013).

4.1 Cisco SGA

Ciscon Security Group Access (SGA) on ratkaisu jolla voidaan luoda pilviä luotetuista tietoverkkolaitteista rakentaakseen turvallisen tietoverkon. Jokainen laite Ciscon SGA pilvessä on autentikoitu muilla ennalta tunnetuilla laitteilla. Kommunikointi laitteiden välillä SGA pilvessä on turvattu monilla kryptaus-menetelmillä, pakettien eheystarkastuksilla ja data-path replay suojausmekanismilla. SGA ratkaisu käyttää laitteen ja käyttäjän identiteettitietoja, jotka saadaan autentikoinnin aikana luokitellakseen paketit laitteen kytkeytyessä verkkoon. Pakettien luokittelu on hallittu laittamalla paketteihin tunnisteita niiden liittyessä kyseiseen verkkoon, jotta ne voidaan tunnistaa asianmukaisesti lisätäkseen suojausta ja muita menettelyjä ennalta määriteltyjen kriteereiden perustein. Käytettävää tunnistetta kutsutaan turvallisuustunnisteeksi (SGT) (Cisco, 2017).

4.2 Cisco ACE

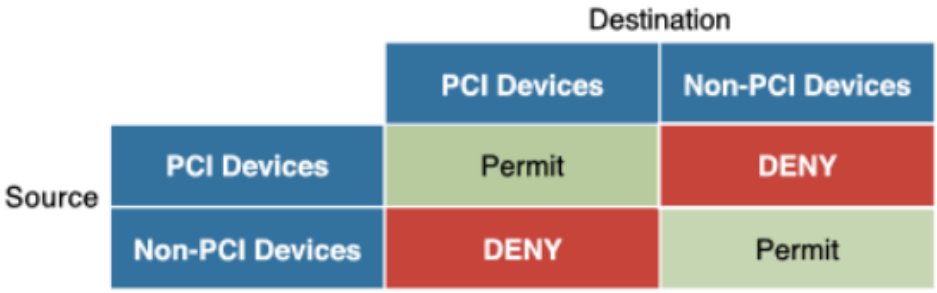
Cisco TrustSecista puhutaan seuraavan generaation vahvistetusta kulunvalvonnasta(Access Control Enfrocement, ACE) ja segmentointi teknologiasta. TrustSecin tarkoituksena on käsitellä huolenaiheita liittyen kasvaviin perinteisiin käyttöoikeuslistoihin ja palomuurien sääntöihin. TrustSec käyttää suojattua ryhmäoikeutta(SGA), suojattu ryhmäoikeus ei täytä TCAMia (Ternary Content Addressable Memory) toisin kuin perinteinen käyttöoikeuslista (Cisco 2017).

4.3 Cisco SXP

Cisco on kehittänyt protokollan jolla mahdollistetaan TrustSecin käyttö laitteilla, jotka suoranaisesti eivät tue kyseistä tekniikkaa sellaisenaan. SGT Exchange Protocol on hallinnointiprotokolla, jolla saadaan IP-to-SGT muokkaus aikaiseksi, eli IP-osoite sidotaan tiettyyn turvallisuustunnisteeseen laitteen ollessa sellainen joka ei pysty lisäämään tunnisteita paketteihin. Päämäärän autentikointi tapahtuu seuraavasti, käyttäjän edetessä ennalta määritetyllä Ciscon TrustSec IP-osoitteella, on kyseiseen osoitteeseen lisätty turvallisuustunniste päätelaitteen perustein DHCP selvityksen avulla ja IP-laite seurannalla. Laite jolla yritetään luoda yhteys lähettää siihen liittyvän tiedon protokollan läpi Cisco TrustSec yhteensopivalle laitteelle. Näillä laitteilla mahdollistetaan ja hallitaan luetteloa kaikista IP-osoitteesta turvallisuustunnisteeksi tapahtuvaa muutosta ja niiden tunnistusta. Paketit suodatetaan ulommalla rajapinnalla, jossa Cisco TrustSec yhteensopiva päätelaite toimii, lisäämällä niihin tieto kyseisestä luettelosta (Cisco, 2016).

4.4 Cisco TrustSec PCI-rajaus

Seuraavassa kuvassa (KUVA 2) näytetään kuinka Cisco TrustSec menettelee eri kohteiden välillä riippuen käyttöoikeuksista.



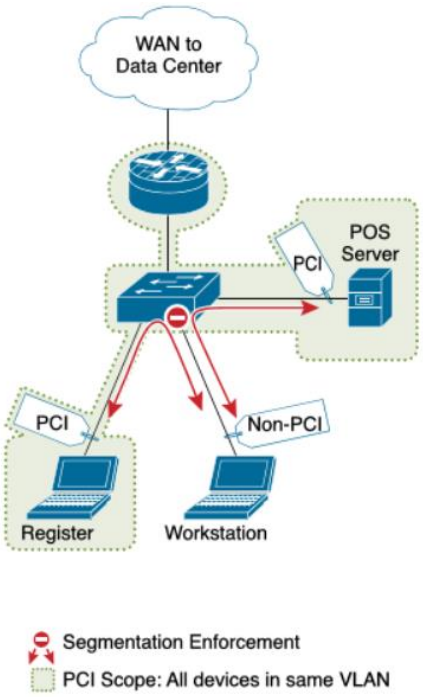
KUVA 2. TrustSec menettely käyttöoikeuksien perusteella.(Cisco TrustSec for PCI Scope Reduction, 2014, Cisco Systems)

Kuvassa (KUVA 2) vasemmassa reunassa on lähteenä toimiva päätelaite ja yläreunassa määränpäänä toimiva päätelaite. Yllä olevassa esityksessä nähdään kuinka maksukorttitietoja käsittelevä laite lähteenä saa ainoastaan yhteyden maksukorttitietoja käsittelevään päätelaitteeseen. Sama tapahtuu kun vaihdetaan lähteeksi päätelaite joka ei käsittele maksukorttitietoja saa yhteyden ainoastaa samankaltaiseen laitteeseen. Eri segmenttien sisällä

olevien laitteiden kommunikaatio on evätty kokonaan, koska näiden välillä ei ole mitään syytä keskustella keskenään.

4.4.1 Käyttö johdotetussa ympäristössä

Alla olevassa esityksessä on näytetty kuinka maksukorttitietoja käsittelevien laitteiden rajaus on toteutettu fyysisesti johdotetun tietoverkon sisällä.

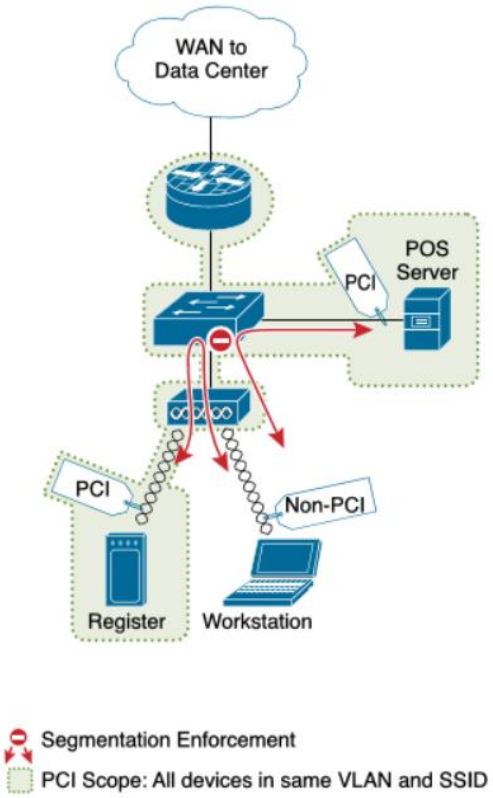


KUVA 3. PCI rajaus fyysisesti johdotetussa ympäristössä. (Cisco TrustSec for PCI Scope Reduction, 2014, Cisco Systems)

Kaikki laitteet ovat liitettynä samaan aliverkkoon VLAN 10. Vasemmassa alareunassa nähdään kassarekisteri ja oikeassa reunassa POS-serveri, jotka ovat luokiteltu ”PCI” suojattuun ryhmään ja niille on annettu ryhmän sisällä olevat turvallisuustunnisteet. Kuvassa (KUVA 3) on myös työpiste, joka ei kuulu tähän samaan ryhmään, joten siltä puuttuu vastaava turvallisuustunniste. Kassarekisteri pystyy kommunikoimaan serverin ja datakeskuksen kanssa, mutta kassarekisteri ei voi muodostaa yhteyttä työpisteen kanssa. Työpiste voi siis ainoastaan kommunikoida kyseissä verkossa ainoastaan datakeskuksen kanssa, serverin ja kassarekisterin kanssa kaikki kommunikaatio on evätty (Cisco, 2014).

4.4.2 Käyttö langattomassa ympäristössä

Seuraavassa esityksessä on näytetty kuinka maksukorttitietoja käsittelevien laitteiden rajaus on toteutettu langattoman tietoverkon sisällä.

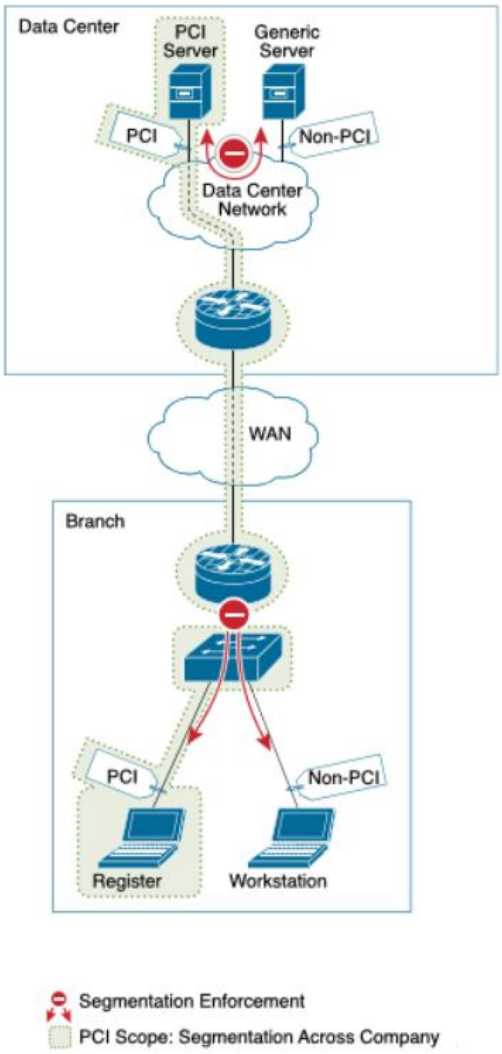


KUVA 4. PCI rajaus langattomassa ympäristössä. (Cisco TrustSec for PCI Scope Reduction, 2014, Cisco Systems)

Kaikki kuvassa (KUVA 4) näkyvät laitteet ovat samassa aliverkossa VLAN 10. Langattomat laitteet käyttävät samaa langattoman lähiverkon verkkotunnusta(SSID). Vasemmassa alareunassa nähdään langaton kassarekisteri ja oikeassa reunassa POS-serveri, jotka ovat luokiteltu ”PCI” suojattuun ryhmään ja niille on annettu ryhmän sisällä olevat turvallisuustunnisteet. Langattomalla työpisteellä ei ole turvallisuustunnistetta, joten se pystyy ainoastaan luomaan yhteyden datakeskuksen välille. Vuorostaan samaan PCI-rajaukseen kuuluvat kassarekisteri ja POS-serveri voivat kommunikoida toistensa kanssa, mutta eivät langattoman työpisteen kanssa (Cisco, 2014).

4.4.3 Käyttö useamman tietoverkon välillä

Viimeisessä esityksessä on näytetty kuinka maksukorttitietoja käsittelevien laitteiden rajaus on toteutettu useamman tietoverkon sisällä.



KUVA 5. PCI rajaus useamman tietoverkon sisällä. (Cisco TrustSec for PCI Scope Reduction, 2014, Cisco Systems)

Kuva (KUVA 5) esittää kuinka tehokkaasti segmentointi voi tapahtua useamman tietoverkon välillä. Esityksen alareunassa nähdään yrityksen toimipiste, jossa nähdään kassarekisteri vasemmalla ja oikealla työpiste. Ylemmässä osassa nähdään yrityksen datakeskus, jossa ovat PCI-serveri ja yleinen serveri. PCI-serveri ja kassarekisteri kuuluvat PCI-rajauksen alle ja omaavat turvallisuustunnisteen. Informaatio jolla luokitellaan verkkoon kuuluvia laitteita jaetaan toimipisteen ja datakeskuksen välillä. Yleinen serveri ja työpiste eivät omaa turvallisuustunnistetta, joten ne voivat kommunikoida ainoastaan keskenään, mutta eivät voi luoda yhteyttä PCI-rajauksen sisällä oleviin laitteisiin. PCI-serveri ja kassarekisteri voivat luoda yhteyden toisiinsa, mutta kommunikointi on evätty PCI-rajauksen ulkopuolella oleviin laitteisiin (Cisco, 2014).

4.5 Security Group Tagging(SGT)

Ciscon Security Group Tag(SGT) on teknologia, osa Ciscon SGA ja TrustSec arkkitehtuuria, joka häivyttää puutteet jotka ilmenevät perinteisissä menettelytapojen hallinnollisissa lähestymistavoissa. Käyttäjän kytkeytyessä verkkoon ja yrittäessään päästä käsiksi resurssiin verkon sisällä, Ciscon käyttöoikeuskytkin automaattisesti profiloi käyttäjän ja etsii käyttäjän identifioivan tunnisteen, laite jota käytetään, sekä paikantaa käyttäjän sijainnin ja kellonajan. Kytkin lisää käyttäjän päätelaitteelta lähettämään dataan tunnisteen joka pohjautuu käyttäjälle ennalta määritetyn käyttöoikeuden mukaan. Tunniste on numeerinen arvo, joka on asetettu joko manuaalisesti käyttöoikeuskytkimeen tai automaattisesti hallinnoitu Ciscon Identity Services Engine(ISE) applikaation kautta. Jos käytössä on Ciscon ISE, tunnistetiedot lähetetään jokaiseen teknologialla tuettuun Cisco laitteeseen verkon sisällä.

TrustSec käyttää 16-bittistä turvallisuustunnistetta(SGT) (KUVA 2) luokitellaakseen dataliikenteen, lähde- ja määränpää-IP osoitteen sijaan. Turvallisuustunnistetta voidaan käyttää kun käyttäjä sisäänkirjautuu tilitiedoillansa tai päätelaiteden autentikoidessa liittymäänsä tietoverkkoon. Turvallisuustunniste katsotaan olevan osa OSI-mallin toista kerrosta ja liitetään Ciscon Meta Dataan(CMD) jokaiseen kehykseen tietyissä sessioissa. OSI-mallin toisen kerroksen salausta MACSec 802.1AE voidaan vapaaehtoisesti käyttää kehysten salaukseen kytkimien välillä. Cisco Identity Services Engineä(ISE) voidaan käyttää lisäämään turvallisuustunnisteita verkkolaitteisiin, jotka vahvistaisivat laitteen ulosmeno rajapintaa. Tärkeää on ymmärtää että TrustSec ei toimi lähde- ja määränpää IP-osoitteiden avulla vaan turvallisuustunnisteiden (Kelvin, Cisco Security Solution Engineer 2017).

KUVA 2. SGT lisättynä Ethernet-kehykseen. (Cisco Trustsec & Security Group Tagging, 2014)

5 POHDINTA

Tutkielman tarkoituksena oli selventää Ciscon teknologian hyötyjä tietoverkon turvalliseen segmentoimiseen ja tietoturvan parantamiseen. Tutkielman edetessä huomattiin kuinka tietoverkon segmentoiminen on monimutkaista ja varsinkin kun yrityksellä on tavoitteena laajentaa toimipisteitä. Tietoturvan parannus ja päivittäminen on huomioitu todella isoksi kustannukseksi, joten Ciscon teknologia on tuotu myös esille olevan yhteensopiva jopa laitteiden kanssa jotka eivät suoranaisesti tue kyseistä teknologiaa, ilman että yrityksen tietoverkon infrastruktuuri täytyisi täysin muokata vastaamaan tämän päivän laitteistoja ja ohjelmistoja.

Tutkielman tavoitteena on selventää kohta kohdalta maksuvälineliikennettä kontroloivan yrityksen tietoverkon segmentointia ja siihen liittyviä vaatimuksia. Mielestäni tämä tutkielma antaa ymmärryksen ja käsityksen kuinka Ciscon ratkaisu voidaan implementoida omaan tietoverkkoon ja samalla parantaa oman tietoverkon turvallisuutta.

Tutkielman tarkoituksena ei ole pitää kyseistä ratkaisua ainoana tapana tuoda turvallisuutta maksuvälinetietoja käyttävän ja välittävän yrityksen tietoverkkoon. Tarkoituksena on osoittaa kuinka tulevaisuudessa tietoturvan hallinnointi voi osoittautua todella vaikeaksi hallita ja näillä parannetuilla, sekä uudistetuilla toimintatavoilla, ohjelmistoilla ja palveluilla voidaan turvata yrityksen oman tietoverkon turvallisuutta kasvavassa ja vaativassa ympäristössä.

LÄHTEET

Fisher, Werner. 2017. VLAN basics. Thomas-Krenn. Luettu 3.1.2018. https://www.thomas-krenn.com/en/wiki/VLAN_Basics

Shabeer, ibm. 2014. What is the difference between static VLAN and dynamic VLAN. Luettu 4.1.2018. http://sysnetnotes.blogspot.com/2013/07/what-is-difference-between-static-vlan.html

Cisco TrustSec. 2016. Cisco. Luettu 15.4.2018. https://www.cisco.com/c/en/us/products/security/identity-services-engine/at-a-glance-listing.html

Cisco TrustSec Software-Defined Segmentation At-a-Glance. 2017. Cisco. Luettu 18.4.2018. https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/at-a-glance-listing.html

Cisco TrustSec Policy-Defined Segmentation. 2017. Cisco. Katsottu 18.04.2018. https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/presentation-listing.html

Cisco TrustSec Accelerates and Simplifies Network Security Solution Overview. 2017. Cisco. Luettu 18.4.2018. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution-overview-c22-737173.html

Natalie Timms, Cisco Security Group Access: An Introduction. 2013. Luettu 18.4.2018. https://www.networkcomputing.com/networking/cisco-security-group-access-introduction/1304108564

Cisco. Cisco Identity Services Engine User Guide. 2017. Luettu 18.4.2018. https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_sga_pol.html#46912

eBook: Segment Your Network for Stronger Security. Cisco. 2017.Luettu 18.4.2018. https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html

Piyevsky Sabina. 2015. Rockwell Automation. Logical Segmentation and VLANs-An Overview. Luettu 18.4.2011. http://www.industrial-ip.org/en/industrial-ip/convergence/logical-segmentation-and-vlans-overview

Cisco. 2014. Cisco TrustSec for PCI Scope Reduction – Verizon Assessment and Validation-PDF. Luettu 20.4.2018. https://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/white-paper-listing.html

Software-Defined Segmentation. 2016. Cisco. Katsottu 20.4.2018. http://players.brightcove.net/1384193102001/4J1gMC8ie_default/index.html?videoId=5108350208001

Cisco. 2016. Cisco TrustSec Switch Configuration Guide. Luettu 20.4.2018. https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/sxp_config.html

Virtual LAN Security: weaknesses and countermeasures-PDF. 2013. Rouiller, Steve A. SANS Institute. Luettu 21.4.2018.

Kelvin, Cisco Security Solution Engineer .2017. CCIE Security v5. Luettu 21.4.2018. https://blog.synack.co.uk/2017/06/10/ccie-security-v5-trustsec-notes/